UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/739,219	12/19/2000	Takeshi Shimoyama	1341.1075 (JDH)	8512

21171 7590 01/04/2005

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/739,219	SHIMOYAMA, TAKESHI	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 July 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-16 have been examined.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-4. 6-11, 13-15, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Preneel et al. "Recent developments in the design of conventional cryptographic algorithms" (hereinafter Preneel) in view of Saijo U.S. Pat. No. 6501840 (hereinafter Saijo).

4. As per claim 1, 8, 15, and 16, Preneel discloses a cipher designing apparatus for designing cipher logic of a cipher device that effects cipher or decryption per block by using an F-function for converting input bits to output bits by means of a plurality of S-boxes (Preneel: pages 113-114 section 4.2), said cipher designing apparatus comprising:

a. A selecting unit which selects of said plurality of S-boxes based on a memory capacity of a high-speed referable memory provided to said cipher device (Preneel: pages 113-114 section 4.2).

b. A S-box generating unit which generates a plurality of S-boxes each having the characteristics selected by said selecting unit (Preneel: pages 113-114 section 4.2).

Preneel does not explicitly discloses selecting an input and output bit number of said plurality of S-boxes and generating a plurality of S-boxes each having the input and output bit number. However, Saijo discloses selecting input and output bit number and selecting block cipher algorithms based on the input and output numbers (Saijo: abstract and column 2 line 55 – column 4 line 42: calculate the data size to determine the processing type and algorithm type). It would have been obvious to one having ordinary skill in the art to combine the teachings of Saijo within the system of Preneel because it allows cryptographic functions to perform in a most efficient and secure way based on hardware limitations.

5. As per claim 2 and 9, Preneel as modified discloses the cipher designing apparatus according to claim 1. Preneel as modified further comprising a F-function generating unit which generates an F-function having said plurality of S-boxes generated by said S-box generating unit (Preneel: pages 113-114 section 4.2). S-boxes are Feistel structure algorithms as well known in the art.

6. As per claim 3 and 10, Preneel as modified discloses the cipher designing apparatus according to claim 1. Preneel as modified further discloses wherein said selecting unit selects the input and output bit number of each S-box in such a manner that a sum of sizes of said plurality of S-boxes becomes largest within a memory capacity of a primary cache memory installed in a processor provided to said cipher device (Preneel: pages 113-114 section 4.2 and pages 117-118 section 6: the S-boxes should fit in the fast cache memory).

7. As per claim 4 and 11, Preneel as modified discloses the cipher designing apparatus according to claim 3. Preneel as modified further disclose wherein said selecting unit includes:

a. An input unit which inputs an entire input and output bit number of said block and the memory capacity of said primary cache memory (Preneel: pages 113-114 section 4.2 and pages 117-121 section 6);

b. A tentative decision unit which tentatively decides an input and output number of each S-box by generating an input and output number of each S-box by dividing the entire input and output bit number of said block inputted from said input unit and allocating a remainder to the input and output number of an arbitrary S-box (Saijo: column 2 line 55 - column 4 line 42; Preneel: pages 113-114 section 4.2); and

c. A combining unit which combines the input and output numbers of the S-box tentatively decided by said tentative decision unit within the memory (Saijo: column 2 line 55 - column 4 line 42).

Preneel as modified does not explicitly disclose outputting the input and output number into capacity of said primary cache memory. However, Preneel as modified discloses output the bit numbers into data storage. Therefore, it would have been a design choice to modify the reference to include outputting the bid number to primary cache memory.

8. As per claim 6 and 13, Preneel as modified discloses the cipher designing apparatus according to claim 4, Preneel as modified further discloses said combining unit completes combining of the input and output numbers based on a final value determined by the entire input and output bit number of said block and the memory capacity of said primary cache memory

(Saijo: abstract and column 2 line 55 – column 4 line 42). Although Saijo does not explicitly disclose outputting the memory capacity of said primary cache memory. However, it would be inherent to know the cache memory capacity to try to fit the S-boxes in the fast cache memory (Preneel: pages 113-114 section 4.2).

9. As per claim 7 and 14, Preneel as modified discloses the cipher designing apparatus according to claim 4, Preneel as modified further discloses padding the remainder and process them. Therefore, Preneel as modified further disclose wherein said tentative decision unit tentatively decides the input and output number of each S-box by allocating said remainder, if there is any, to the input and output numbers of the S-boxes that are placed apart at remotest positions (Saijo: column 2 lines 15-39). It is well known in the art to pad a block at the end or remotest positions.

10. Claims 5 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Preneel in view of Saijo and further in view of Luyster U.S. Pat. No. 6182216 (hereinafter Luyster).

11. As per claim 5 and 12, Preneel as modified discloses the cipher designing apparatus according to claim 1. Preneel as modifies further discloses deciding the best block size for certain algorithms (Saijo: column 9 lines 1-62). Preneel as modified does not explicitly disclose a smallest input and output number specifying unit which specifies a smallest value of the input and output number of said plurality of S-boxes. However, Luyster discloses that limitation (Luyster: column 16 lines 38-65). It would have been obvious to one having ordinary skill in the

art to combine the teachings of Luyster within the combination of Preneel-Saijo because it is well known in the art that size affects the efficiency and security of a cryptographic process and a minimum bound is required to maintain satisfactory performance.

Response to Arguments

12. Applicant's arguments filed have been fully considered but they are not persuasive.

13. Regarding to applicant's argument, applicant argues that the references do not teach "based on a memory capacity of a high-speed referable memory provided to said cipher device" and "generates a plurality of S-boxes each having the input and output bit number selected by said selecting unit". However, the Preneel discloses selecting input and output bit number of said plurality of S-boxes based on memory capacity (Preneel: pages 113-114 section 4.2: different algorithm provide different input and output and they should fit in the fast cache memory). Furthermore, Saijo discloses determining the processing and algorithm type based on the calculated data size (Saijo: abstract and column 2 line 55 – column 4 line 42). Therefore, the combination of Preneel and Saijo discloses calculating the input data size to determine the algorithm type and processing type so that different types of S-boxes can be utilized to efficiently perform the cryptographic operation.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Adams et al. U.S. Pat. No. 6031911 discloses generating S-box with desired characteristics and generating S-box based on the size of the input and output (Adams: column 3 line 66 – column 4 line 14).

Kim et al. U.S. Pat. No. 5796837 discloses apparatus and method for generating a secure substitution box immune to cryptanalysis and plurality of S-boxes.

Blaze U.S. Pat. No. 6005944 discloses system and method for constructing block ciphers.

Merkle U.S. Pat. No. 5003597 discloses method and apparatus for data encryption.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC

EMMANUEL L. MOISE
PRIMARY EXAMINER